CLMPTO

AU/2131

01/18/02

Y.M.

Claims

[c1] A network system providing integration, comprising:

a client computer;

a server;

a server-side cryptographic function providing cryptographic services located on the server;

a PKI-Bridge providing an interface between the server and the server-side cryptographic function;

a remote access switch providing an interface between the client computer and the server;

a client-side cryptographic function providing cryptographic services located on the client computer;

a dial-up client providing dialing services to access the remote access switch; and

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function.

Claim2 –

[c2] (Amended) The network system of claim 1, further comprising:

a security device holding authentication information; and

a security device [card] reader attached to the client computer for reading the security device.

Claims 3-13

[c3] The network system of claim 2, wherein a certificate is stored on the security device.

[c4] The network system of claim 2, wherein the security device is a smart card.

[c5] The network system of claim 1, further comprising:
a directory service accessed by the server-side cryptographic function.

[c6] The network system of claim 5, wherein the directory service is lightweight directory access protocol compliant.

[c7] The network system of claim 1, wherein the client-side cryptographic function and the server-side cryptographic function employ the same cryptographic scheme.

[c8] The network system of claim 1, wherein the server-side cryptographic function uses a random number generator to generate a challenge string.

[c9] The network system of claim 1, wherein a client-side cryptographic function uses a random number generator to generate a response string.

[c10] The network system of claim 1, wherein the client-side cryptographic function generates a signed response string.

[c11] The network system of claim 1, wherein the server-side cryptographic function generates a challenge string.

[c12] The network system of claim 1, wherein the server-side cryptographic function verifies the signed response string.

[c13] The network system of claim 1, wherein the dial-up client operates in terminal mode.

Claim 14

[c14] (Amended) A network system providing integration, comprising:

a client computer;

a server;

a server-side cryptographic function providing cryptographic services located on the server;

a PKI-Bridge providing an interface between the server and the server-side cryptographic function;

a remote access switch providing an interface between the client computer and the server;

a client-side cryptographic function providing cryptographic services located on the client computer;

a dial-up client providing dialing services to access the remote access switch;

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function;

a security device holding authentication information;

a security device [card] reader attached to the client computer for reading the security device; and

a directory service accessed by the server-side cryptographic function.

Claim 15

[c15] A client computer comprising:

a dial-up client providing dialing services to the client computer;

a client-side cryptographic function providing cryptographic services located on the client computer; and

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function.

Claim 16

[c16] (Amended) The client computer of claim 15, further comprising:

a security device [card] reader attached to the client computer for reading a security device.

Claim 17

[c17] The client computer of claim 15, wherein a security device is a smart card.

Claim 18

[c18] (Amended) The client computer of claim 15, wherein the custom script dynamically linked library [dial-up client] comprises a SDLogin component and a SDSetupDial component.

Claim 19

[c19] The client computer of claim 15, wherein the dial-up client automates the authentication process using a hidden terminal operating in terminal mode.

Claim 20

[c20] (Amended) A client computer comprising:

a dial-up client providing dialing services to the client computer;

a client-side cryptographic function providing cryptographic services located on the client computer;

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function; and

a security device [card] reader attached to the client computer for reading a security device.

Claim 21-23

[c21] A server comprising:

a server-side cryptographic function providing cryptographic services located on the server; and

a PKI-Bridge providing an interface between the server and the server-side cryptographic function.

[c22] The server of claim 21, further comprising:

a directory service accessed by the server-side cryptographic function.

[c23] A server comprising:

a server-side cryptographic function providing cryptographic services located on the server;

a PKI-Bridge providing an interface between the server and the server-side cryptographic function; and

a directory service accessed by the server-side cryptographic function.

Claim 24-25

[c24] (Amended) A method of integrating via a dial-up interface, comprising:

sending session initiation information from a dial-up client to a PKI-Bridge;

checking session initiation information by the PKI-Bridge;

generating a challenge string by a server-side cryptographic function;

forwarding the challenge string to a custom script dynamically linked library;

forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;

utilizing [retrieving] a private key from a security device;

generating a response string;

signing the response string with the private key of a dial-in user;

forwarding a signed response string to the custom script dynamically linked library;

dividing the signed response string into packets;

forwarding packets to the PKI-Bridge;

reconstructing the signed response string from packets;

forwarding a reconstructed signed response string to the server-side cryptographic function;

obtaining a public key of the dial-in user; and

verifying the reconstructed signed response string using the server-side cryptographic function.

[c25] (Amended) The method of claim 24, further comprising:

reading the security device by a security device [card] reader.

Claim 26-33

[c26] The method of claim 24, further comprising:
encoding the signed response string.

[c27] The method of claim 24, further comprising:
decoding the signed response string.

[c28] The method of claim 24, further comprising:
forwarding the challenge string to the dial-up client; and
forwarding the challenge string to the PKI-Bridge.

[c29] The method of claim 24, further comprising:
forwarding packets from the custom script dynamically linked library.

[c30] The method of claim 24, wherein the security device is a smart card.

[c31] The method of claim 24, wherein the session initiation information comprises version information and a distinguished name.

[c32] The method of claim 24, wherein the public key is stored on a directory service.

[c33] The method of claim 32, wherein the directory service is lightweight directory access protocol compliant.

Claim 34-35

[c34] (Amended) A method of integrating via a dial-up interface, comprising:

sending session initiation information from a dial-up client to a PKI-Bridge;

checking session initiation information by the PKI-Bridge;

generating a challenge string by a server-side cryptographic function;

forwarding the challenge string to a custom script dynamically linked library;

forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;

utilizing [retrieving] a private key from a security device;

generating a response string;

signing the response string with the private key of a dial-in user;

forwarding a signed response string to the custom script dynamically linked library;

dividing the signed response string into packets;

forwarding packets to the PKI-Bridge;

reconstructing the signed response string from packets;

forwarding a reconstructed signed response string to the server-side cryptographic function;

obtaining a public key of the dial-in user;

verifying the reconstructed signed response string using the server-side cryptographic function;

reading the security device by a security device [card] reader;

encoding the signed response string;

decoding the signed response string;

forwarding the challenge string to the dial-up client;

forwarding the challenge string to the PKI-Bridge; and

forwarding packets from the custom script dynamically linked library.

[c35] (Amended) An apparatus of integrating via a dial-up interface, comprising:

means for sending session initiation information from a dial-up client to a PKI-Bridge;

means for checking session initiation information by the PKI-Bridge;

means for generating a challenge string by a server-side cryptographic function;

means for forwarding the challenge string to a custom script dynamically linked library;

means for forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;

means for utilizing [retrieving] a private key from a security device;

means for generating a response string;

means for signing the response string with the private key of a dial-in user;

means for forwarding a signed response string to the custom script dynamically linked library;

means for dividing the signed response string into packets;

means for forwarding packets to the PKI-Bridge;

means for reconstructing the signed response string from packets;

means for forwarding a reconstructed signed response string to the server-side cryptographic function;

means for obtaining a public key of the dial-in user; and

means for verifying the reconstructed signed response string using the server-side cryptographic function.